RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: IDY-M01

Dude, Where's My Password? The Challenges of Getting to Passwordless

Andy Ozment
Chief Technology Risk Officer, Capital One
04/28/2025

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Cybersecurity professionals have bemoaned the use of passwords for years

In 2024,

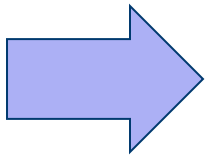
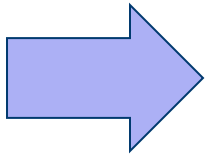
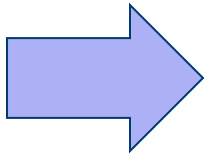
71%

of basic web application attacks leveraged the use of compromised credentials

At Capital One, we are drastically reducing our use of passwords by adopting more secure authentication

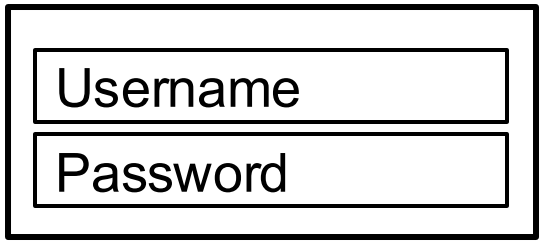
Device certificate + **FIDO2 passkey** = **Passwordless**

Passwordless addresses the flaws of passwords and MFA while advancing the user experience

Attacker obtains password, SMS, or OTP		**Blocked by requirement for hardware authentication**
Attacker tries brute force		**Blocked by requirement for hardware authentication**
Attacker tries man-in-the-middle		**Blocked by asymmetric encryption where no secret is shared**

We've adopted authentication solutions as they have evolved on our journey to passwordless

2005 → **2025**



Andy Ozment

And a huge thank you to the teams who did the actual work in today's presentation:

Enterprise
Programs & Platforms

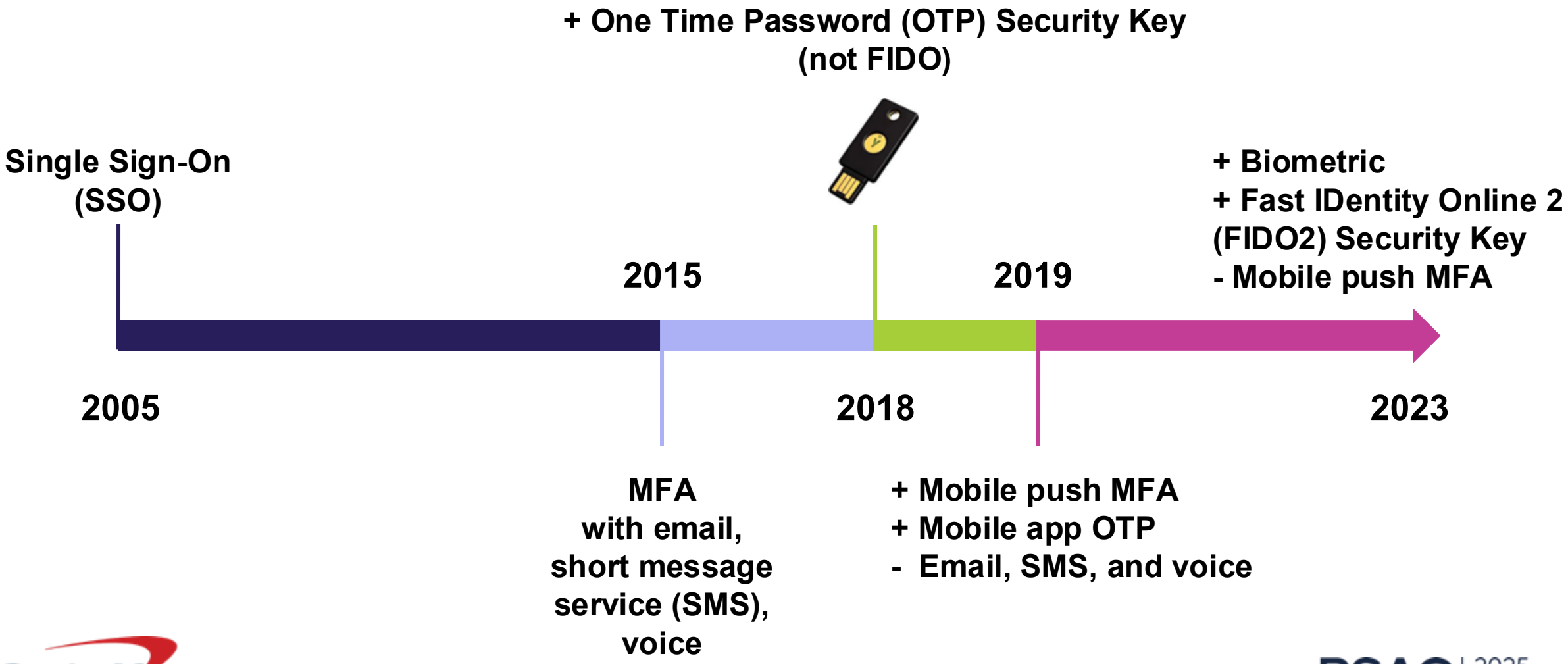
Cyber

Technology
Risk Management

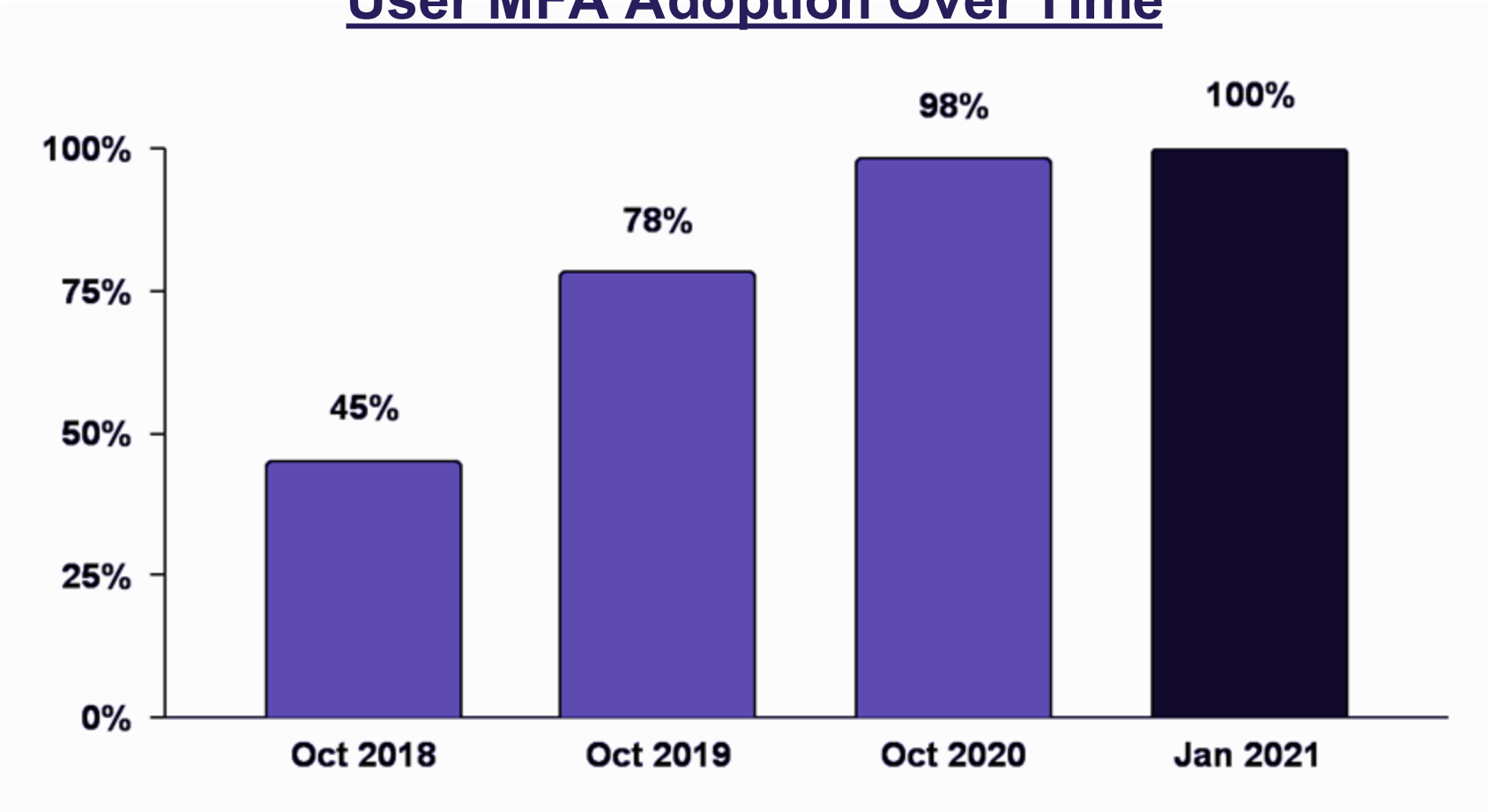
Our journey to passwordless authentication was enabled by going “all in” on the public cloud

We closed our data centers in 2020

To get to passwordless, we first needed to build out our single sign-on and MFA capabilities

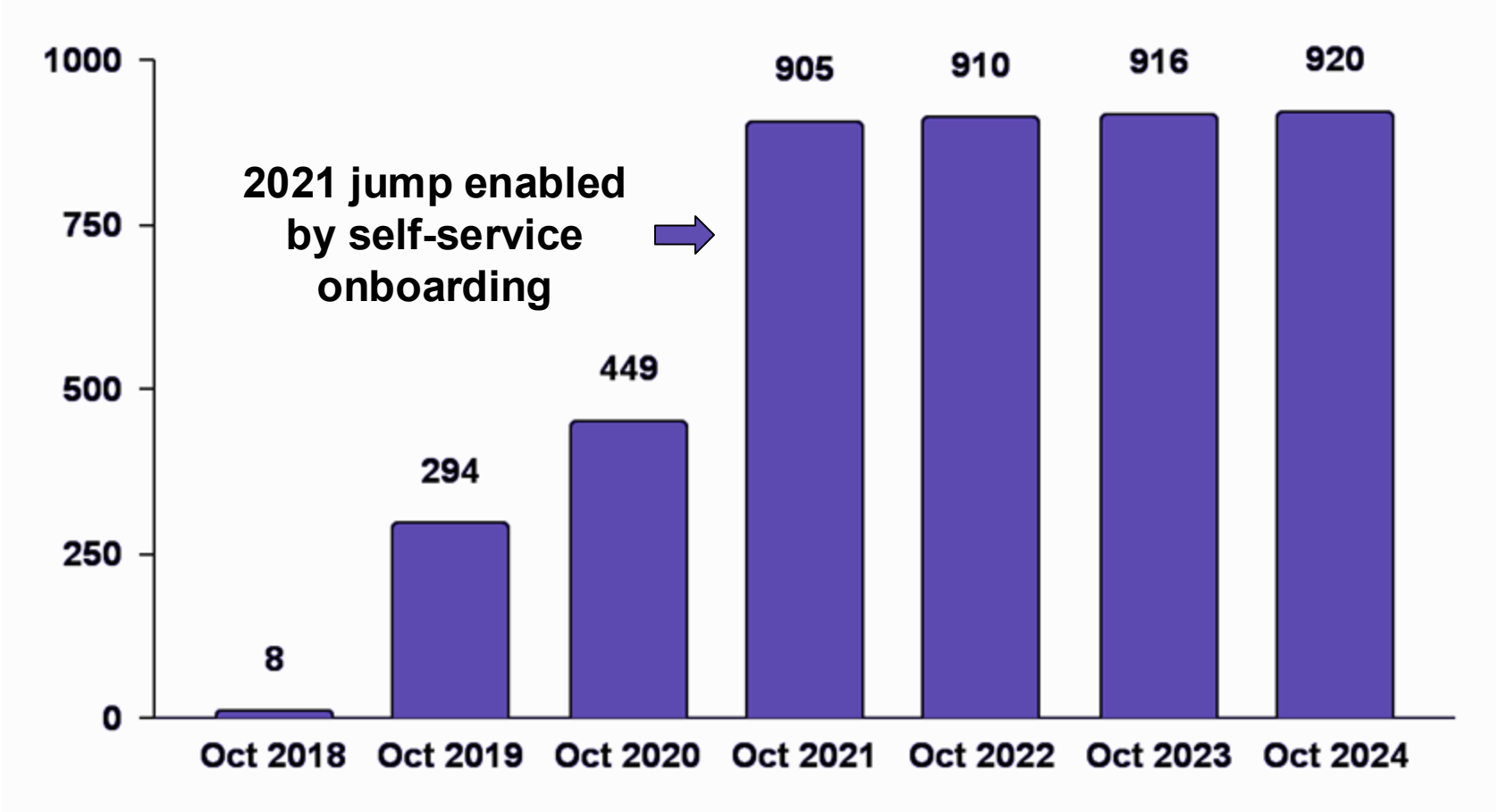


We needed to lay the groundwork in our MFA infrastructure to enable passwordless

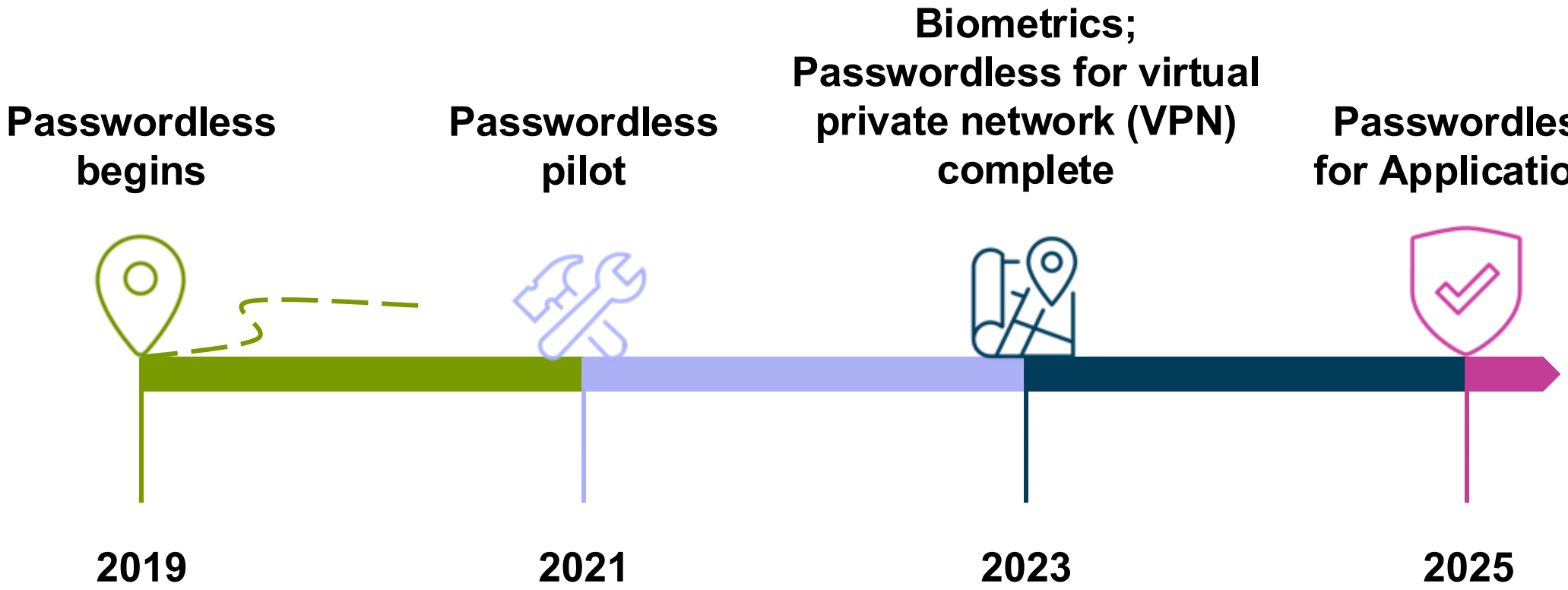


In addition to our users, we also needed to enable our applications for MFA

Application MFA Adoption Over Time



Our final push to passwordless began in 2019



In June 2022, our CISO challenged us to get to Passwordless VPN for employees in one year

June 2023

By the end of 2025, our targeted 1,000+ applications will also require Passwordless for employees

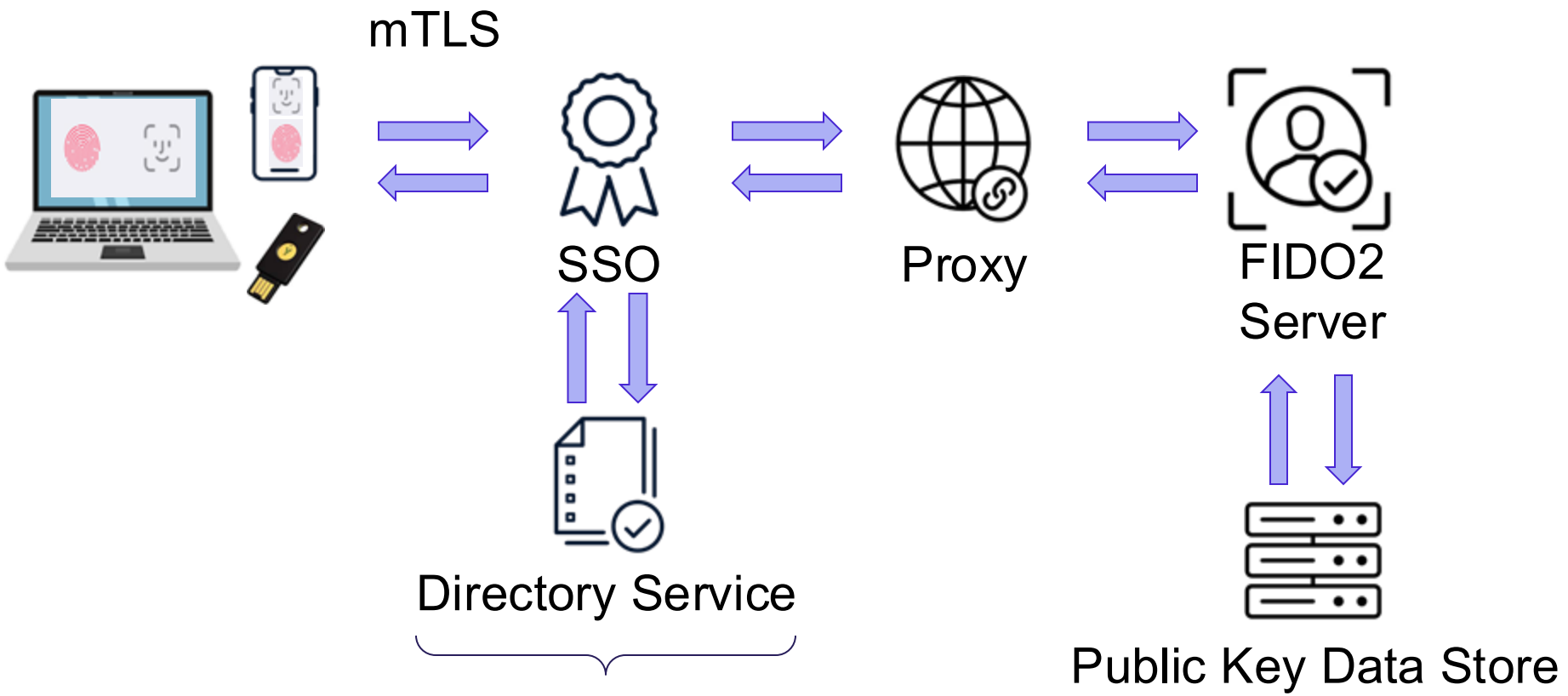
We require modern passkey authentication

Native biometric

OR

Security Key with Personal Identification Number (PIN)

Our architecture is built on modern, open-protocol standards to increase adoption across our apps

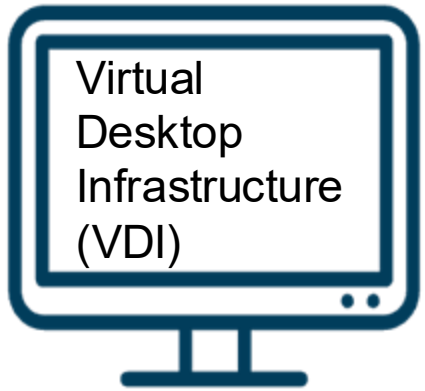


Note: mTLS is Mutual Transport Layer Security, SAML is Security Assertion Markup Language

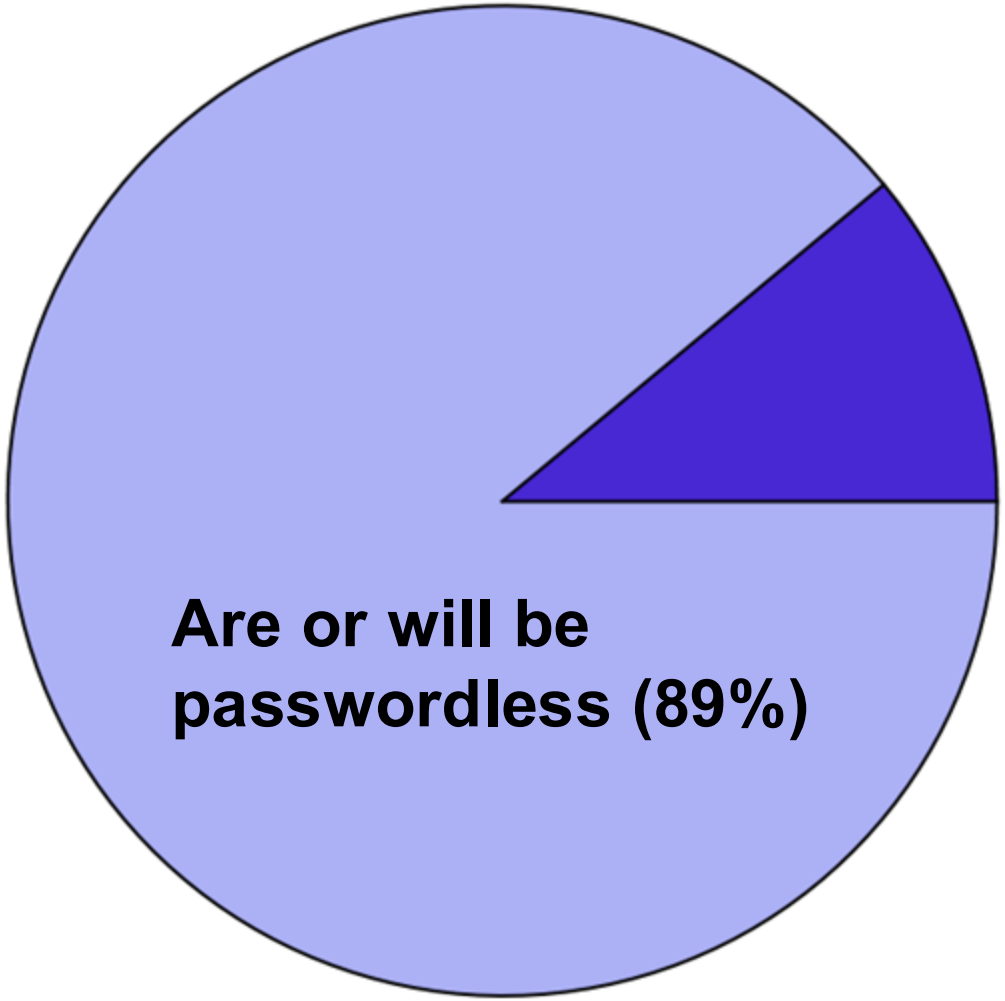
In all cases, we require a corporate-managed device

iOS

Windows



Internal employee apps will almost all be Passwordless



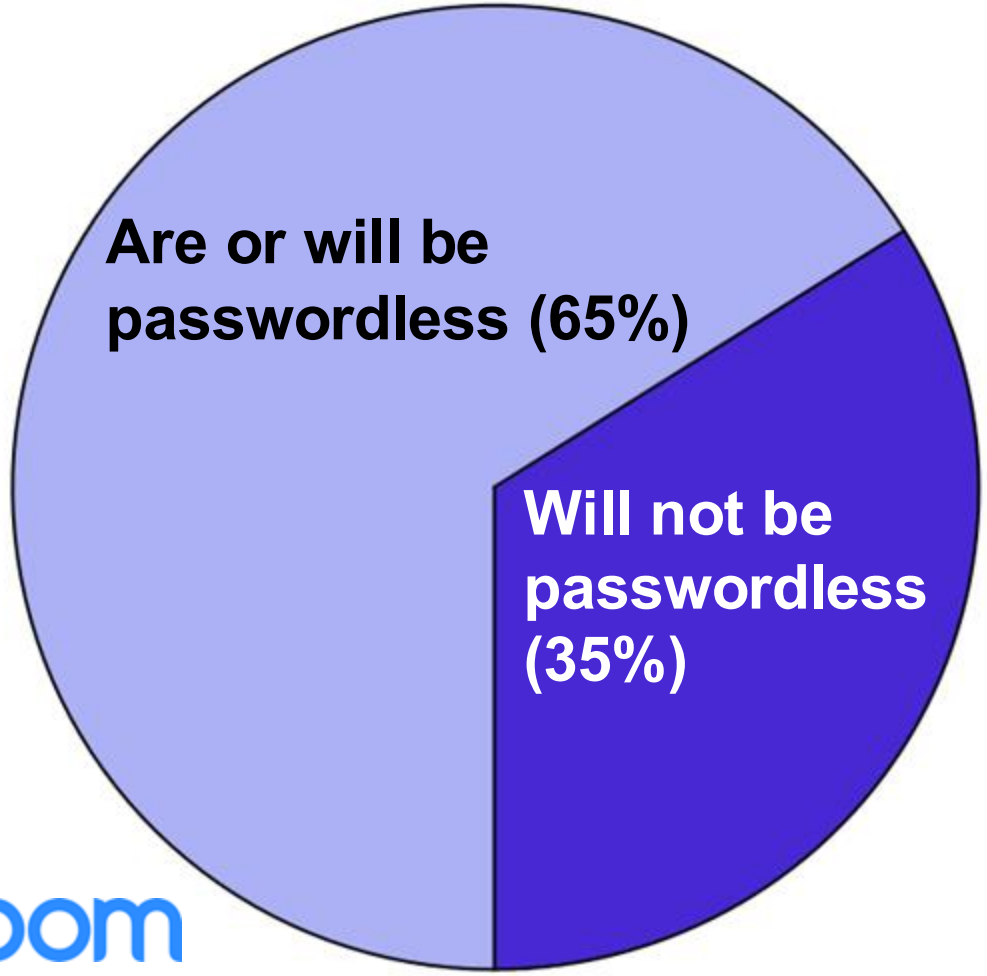
External employee apps will mostly be Passwordless

Internal HR apps

Google Workspace

coursera

zoom



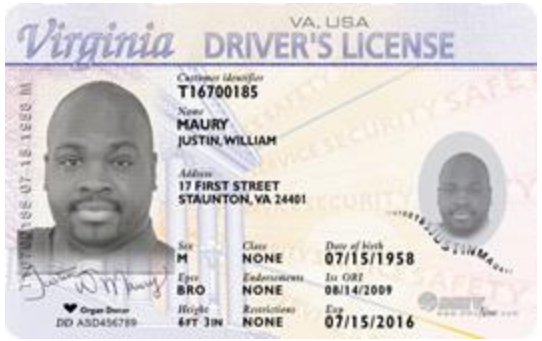
Other external apps

We've learned a lot of lessons on our journey

Identity Proofing

Strong identity verification is crucial when allowing users to register a FIDO2 device for MFA

Government ID Verification via Smartphone

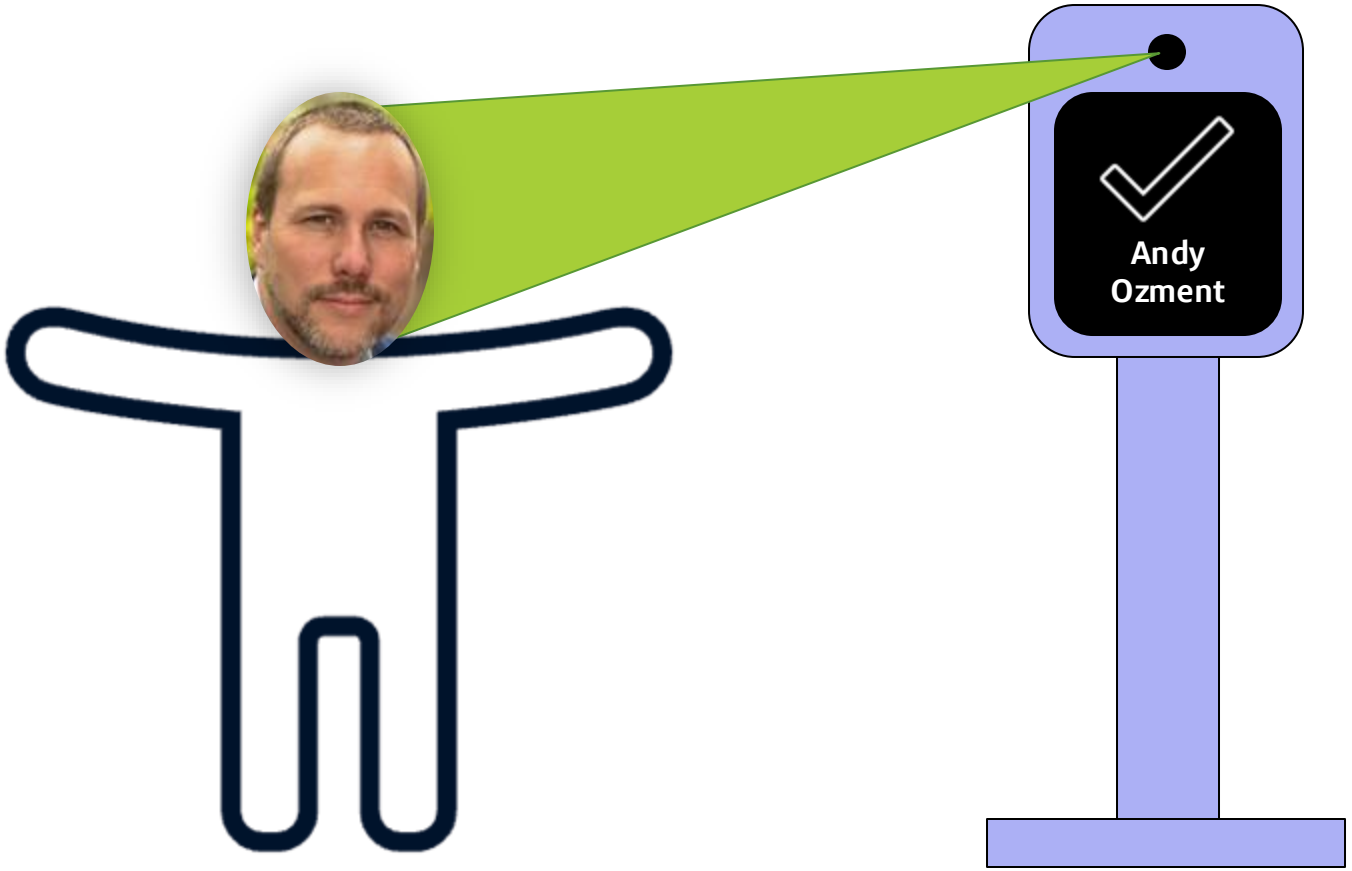


or

Video Verification + One-Time Token

Gen AI makes this approach risky without additional controls

For employees without mobile phones on site, we plan to implement kiosks for identity verification



We've learned a lot of lessons on our journey

Identity Proofing

Interoperability

We've mitigated the risk of iCloud Keychain sync by requiring the use of corporate managed devices

- Non-managed personal device

- Corporate managed device w/ x509 certificate
- Enforcement of mTLS

For our PC users, we accepted a small frequency of failed logins due to tool collisions

0.04%

Our cloud proxy required tuning because it blocked some Microsoft URLs.

A second login attempt resolved most failed logins.

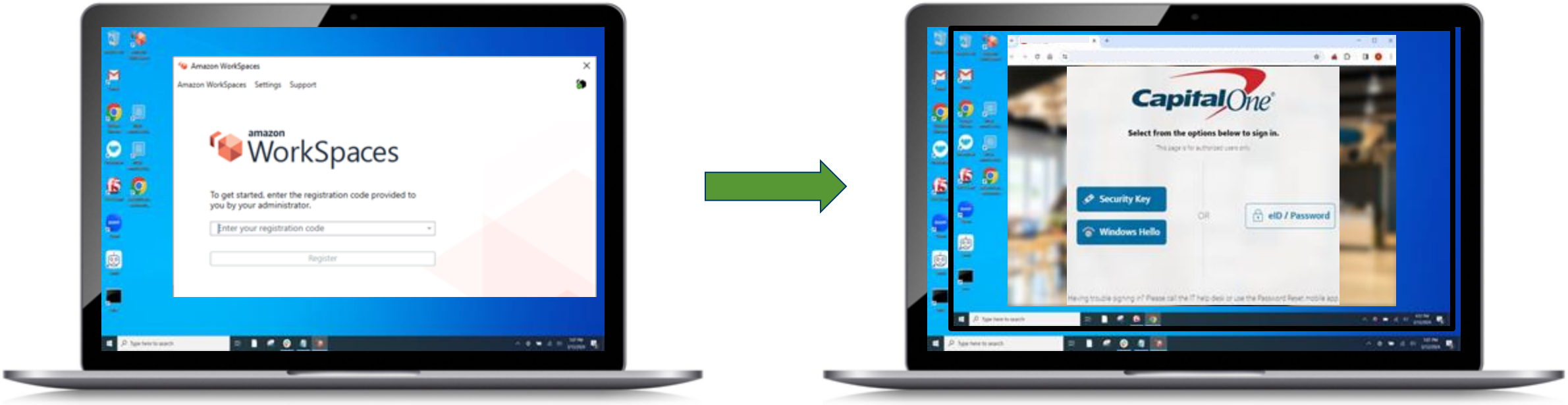
We've learned a lot of lessons on our journey

Identity Proofing

Interoperability

VDI

VDIs represent additional “front doors” for initial authentication that needed to become passwordless



Once logged into the VDI “front door,” internal applications should be passwordless enforced

We needed VDI vendors to enable FIDO2, and they did

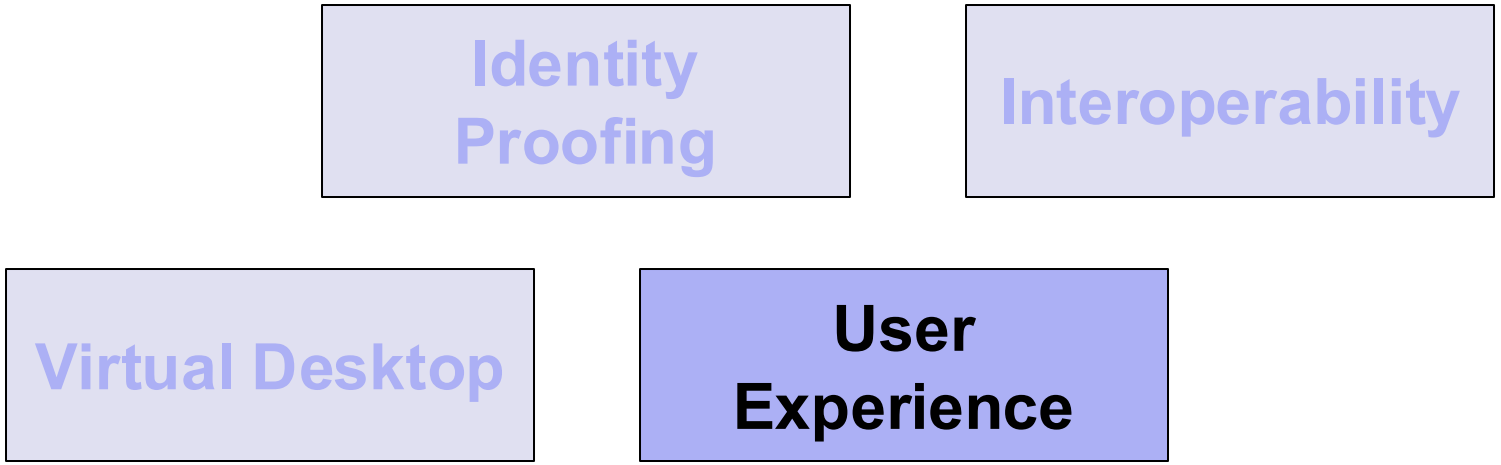
Enabled Sep. 2022

Enabled May 2023

Enabled Oct. 2023

Enabled Mar. 2024

We've learned a lot of lessons on our journey



Our internal branding played a critical role in socializing and driving change

"FIDO2"
jargon / too technical

"MFA"
technically, already in place

"Passwordless"

- ✓ Unique in our internal brand names
- ✓ Described users' experience
- ✓ Easiest to understand

Security Keys were rolled out to the enterprise as MFA devices in 2019 in OTP mode

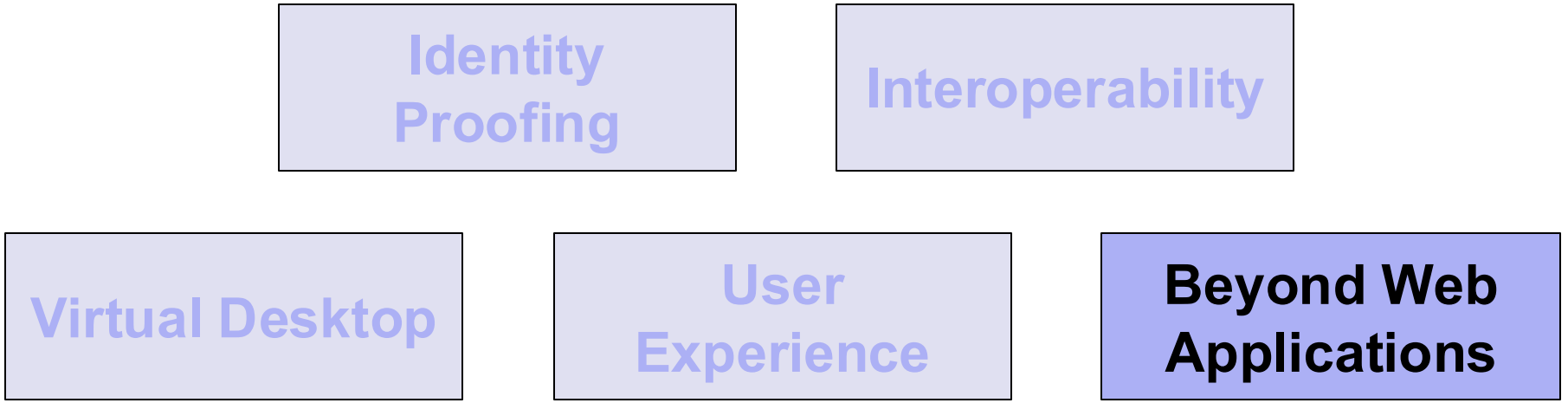
Primarily deployed Security Keys that supported both OTP and FIDO2

This allow OTP while we transition to a fully passwordless FIDO2 environment

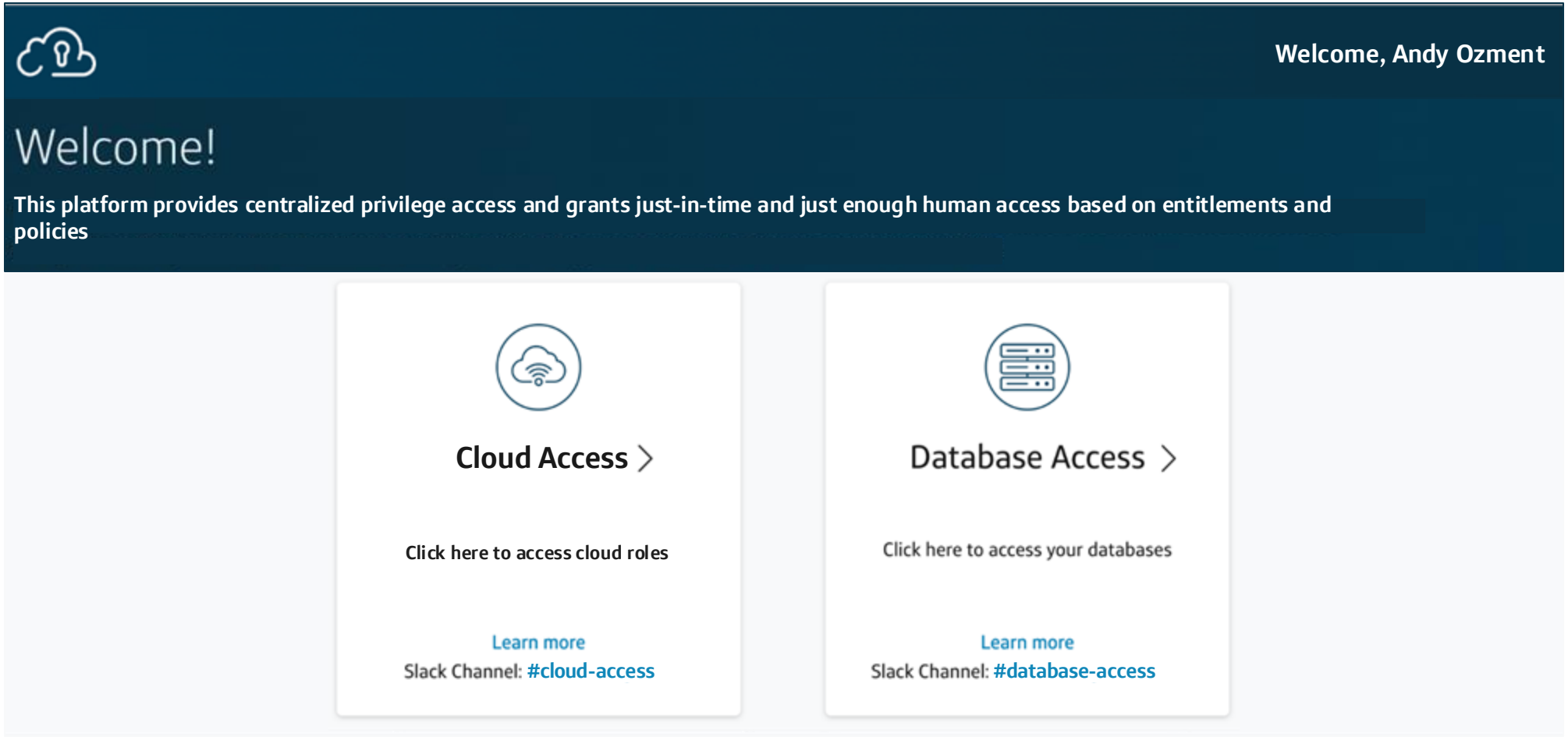
Despite our best efforts, employees were confused with what passwordless was—and was not

1. People were used to using Security Keys in OTP mode
2. Introducing “Security Key” using the exact same device was confusing, people struggled to understand the difference
3. Kept it simple by spelling out “Passwordless” and “Not-Passwordless” for each option (Security Key and Security Key OTP respectively)

We've learned a lot of lessons on our journey



Beyond web applications, we are mandating passwordless on databases and consoles


Welcome, Andy Ozment
Welcome!
This platform provides centralized privilege access and grants just-in-time and just enough human access based on entitlements and policies
Cloud Access
Click here to access cloud roles
Learn more
Slack Channel: #cloud-access
Database Access
Click here to access your databases
Learn more
Slack Channel: #database-access

We've dramatically reduced our risk while improving our user experience

We started our authentication journey way back in 2005

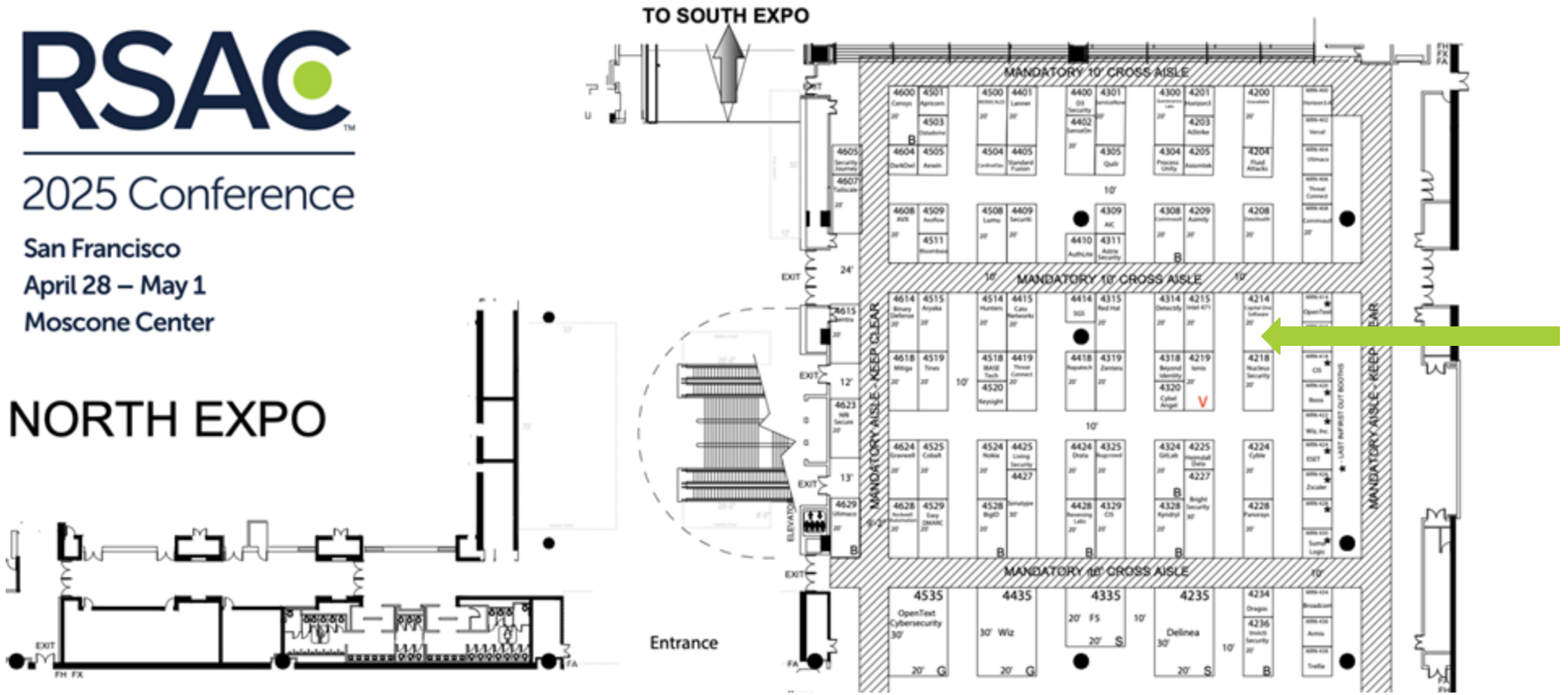
Centralized IAM is key

Change management, including branding and comms, is vital

Success with MFA helps you turn the corner to Passwordless

Apply what you have learned today

- Next week you should:
  - Understand the current state of your identity and authentication services
  - Assess your organization's readiness for Security Key adoption
- In the first three months following this presentation you should:
  - Carefully plan for user experience customization and branding—these will determine success!
  - Centralize IAM authentication services to drive adoption of new assets (i.e. Security Keys)
  - Identify material changes needed in your stack (i.e. SSO and MFA)
  - Identify an identity proofing solution that withstands GenAI risks
  - Identify an approach for exceptions and edge cases, including: BYOD and VDIs
- Within six months you should:
  - Set measurable objectives and timeliness for passwordless adoption within your organization

Q&A

Visit Capital One Software at the expo (N-4214):